Tutorial 3: Proof techniques

Department of Computer Science and Engineering
Hong Kong University of Science and Technology

Question 1

Let a and n be two positive integers. Prove the following statement by contraposition:

> "If there exist integers x and y such that $ax + ny = 1$, then no integer common factor of a and n that is larger than 1."

Solution:
By contraposition, to prove the given statement, it is equivalent for us to prove: If a and n has integer common factor larger than 1, then there is no integer pair (x, y) such that $ax + ny = 1$.

Suppose a and n has an integer common factor $d > 1$, and $a = dp$ and $n = dq$ where p and q are integers. Therefore, $ax + ny = dpx + dqy = d(px + qy)$. No integer pair (x, y) can make $ax + ny$ equal to 1 because $d > 1$ and $(px + qy)$ is an integer.

Question 2

Consider the following definitions:

- $\log_2(n) = x$ if and only if $2^x = n$, and
  $\lfloor \log_2(n) \rfloor = i$ such that $2^i \leq n < 2^{i+1}$.
  e.g., $\lfloor \log_2(2) \rfloor = 1$, $\lfloor \log_2(3) \rfloor = 1$, $\lfloor \log_2(4) \rfloor = 2$, $\lfloor \log_2(31) \rfloor = 4$, $\lfloor \log_2(32) \rfloor = 5$, $\lfloor \log_2(33) \rfloor = 5$
- Prime factorization of n is the representation of n as multiplication of a list of primes.
  e.g. $12 = 2 \cdot 2 \cdot 3, 720 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.
- $SIZE(n)$ represents the number of prime factors in prime factorization of n.
  e.g. $SIZE(12) = 3, SIZE(720) = 7$.

Prove the following statement by contradiction:

"For any positive integer n, $SIZE(n) \leq \lfloor \log_2(n) \rfloor$."

Solution:
Let $P(n)$ denotes $SIZE(n) \leq \lfloor \log_2(n) \rfloor$.
Assume the statement is wrong.
i.e. There is a smallest integer m s.t. $P(m)$ is false.
$P(1)$ is true, because $SIZE(1) = 0 = \lfloor \log_2(1) \rfloor$, so $m > 1$.
Let p be any prime factor of m. Then,

$$\begin{aligned} SIZE(m) &= SIZE((m/p)p) \\ &= SIZE(m/p) + 1 \\ &\leq \lfloor \log_2(m/p) \rfloor + 1 && m/p < m, \text{ so } P(m/p) \text{ is true} \\ &\leq \lfloor \log_2(m/2) \rfloor + 1 \\ &\leq \lfloor \log_2(m) \rfloor \end{aligned}$$

This contradicts with our assumption.

Question 3

Prove the following statement by contradiction and contraposition:

"For any integer x, if $x^3 - 4x + 3$ is even, then x is odd."

Solution:

Prove by contradiction:

Assume there exist some integers x s.t. $x^3 - 4x + 3$ and x are even.
We have $x = 2k$ for some integer k, and thus
$x^3 - 4x + 3 = 8k^3 - 8k + 3 = 2(4k^3 - 4k + 1) + 1$ which is odd.
This contradicts with our assumption that $x^3 - 4x + 3$ and x are even for some integers x.

Prove by contraposition:

For any even integer x, we have $x = 2k$ for some integer k.
This implies that
$x^3 - 4x + 3 = 8k^3 - 8k + 3 = 2(4k^3 - 4k + 1) + 1$ is odd.
By the contrapositive rule, the statement is proved.